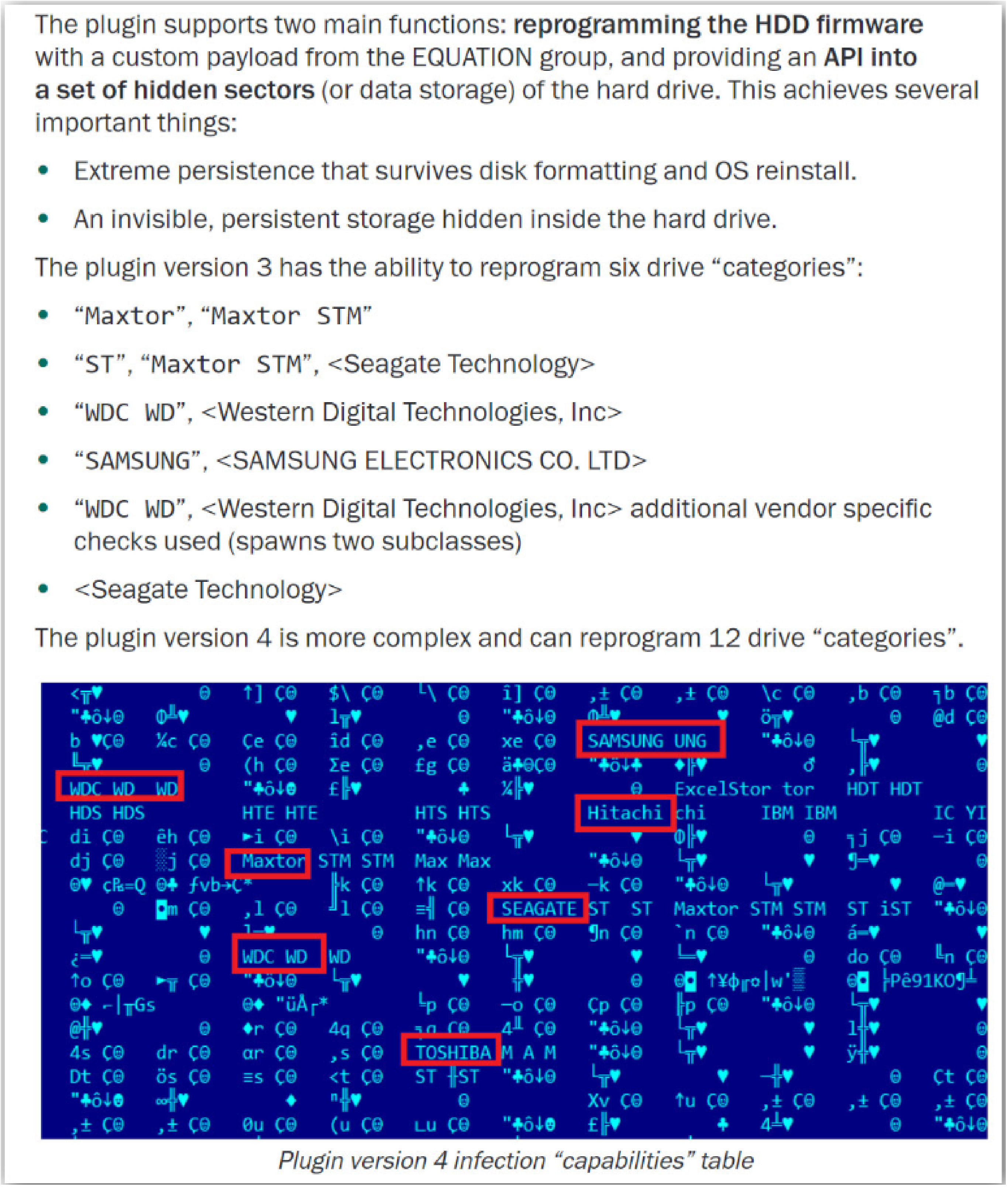
GIGABYTE Driver Exploited By Ransomware To Kill AV Processes



The plugin supports two main functions: **reprogramming the HDD firmware** with a custom payload from the EQUATION group, and providing an **API into a set of hidden sectors** (or data storage) of the hard drive. This achieves several important things:

- Extreme persistence that survives disk formatting and OS reinstall.
- An invisible, persistent storage hidden inside the hard drive.

The plugin version 3 has the ability to reprogram six drive “categories”:

- “Maxtor”, “Maxtor STM”
- “ST”, “Maxtor STM”, <Seagate Technology>
- “WDC WD”, <Western Digital Technologies, Inc>
- “SAMSUNG”, <SAMSUNG ELECTRONICS CO. LTD>
- “WDC WD”, <Western Digital Technologies, Inc> additional vendor specific checks used (spawns two subclasses)
- <Seagate Technology>

The plugin version 4 is more complex and can reprogram 12 drive “categories”.

Plugin version 4 infection “capabilities” table

GIGABYTE Driver Exploited By Ransomware To Kill AV Processes

Download

Ransomware Exploits GIGABYTE Driver to Kill AV Processes (BleepingComputer) The attackers behind the RobbinHood Ransomware are .... The attackers behind the RobbinHood Ransomware are exploiting a vulnerable GIGABYTE driver to install a malicious and unsigned driver .... This second driver then goes to great lengths to kill processes and files ... we've only seen the Gigabyte driver being abused in this way.

Cyber News - Check out top news and articles about cyber security, malware attack updates and more at Cyware.com. Our machine learning .... Ransomware Exploits GIGABYTE Driver to Kill AV Processes February 6, 2020- Bleeping Computer. The attackers behind the RobbinHood Ransomware a.. GIGABYTE Driver exploited by ransomware to kill AV Processes - SecurityNewsWire.com for cyber security news, latest IT security news, cyber security threat .... RobbinHood ransomware exploit GIGABYTE driver flaw to kill ... are exploiting a vulnerable GIGABYTE driver to kill antivirus products. ... Normally, Windows security software processes could only be killed by Kernel drivers.. In this case, the ransomware exploits this vulnerability in order to kill running ... However, a driver created by Gigabyte, the well-known Taiwanese ... list of security product processes to terminate and then it deletes the files ... PureLocker Multiplatform Ransomware Avoids Legacy AntiVirus Detection ...

Integrated to-do list tool

The RobbinHood ransomware is using a deprecated Gigabyte driver as the tip of the spear for taking out antivirus products. ... Once that's loaded, they can then exploit that driver using the known vulnerability in order to load ... Killing such security processes from kernel mode offers plenty of upside for the .... 07-02-2020 GIGABYTE Driver exploited by ransomware to kill AV Processes. 07-02-2020 Chinese hacking campaign warning by Malaysia government.. WannaCry ransomware attack on NHS could have triggered NATO reaction, says ... Specifically, RobbinHood loads the Gigabyte driver, exploits the ... and then instructs it to kill off the processes and files of antivirus products, ... koszulki vista

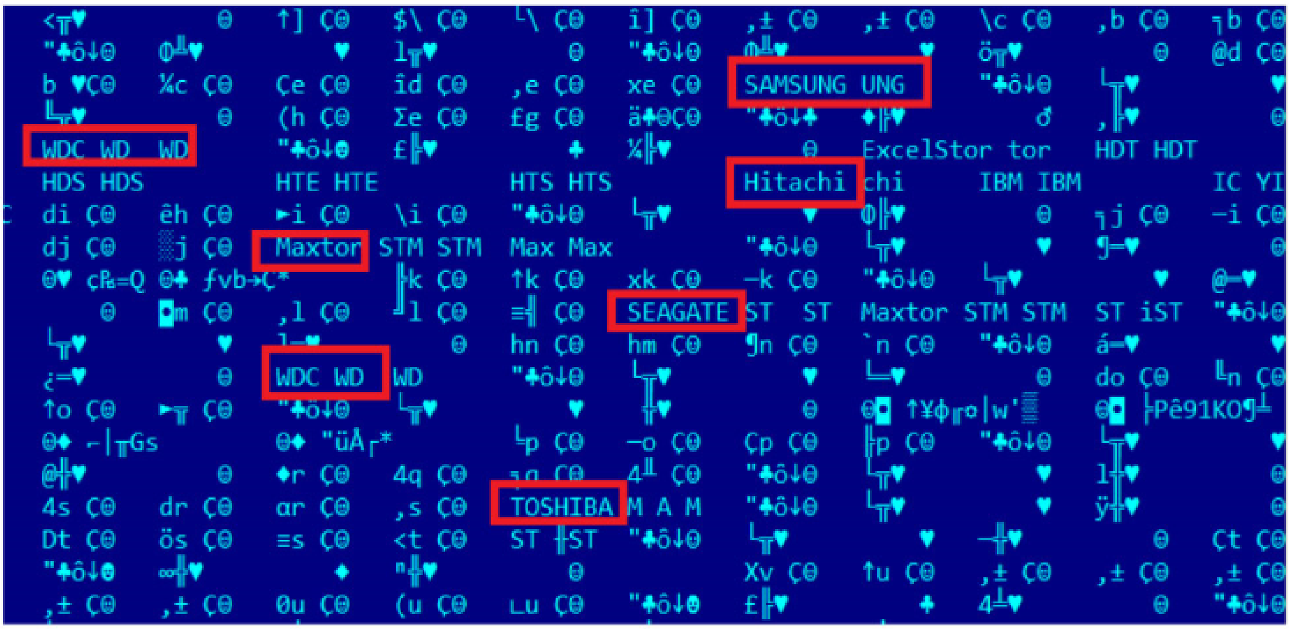
The plugin supports two main functions: **reprogramming the HDD firmware** with a custom payload from the EQUATION group, and providing an **API into a set of hidden sectors** (or data storage) of the hard drive. This achieves several important things:

- Extreme persistence that survives disk formatting and OS reinstall.
- An invisible, persistent storage hidden inside the hard drive.

The plugin version 3 has the ability to reprogram six drive "categories":

- "`Maxtor`", "`Maxtor STM`"
- "`ST`", "`Maxtor STM`", <Seagate Technology>
- "`WDC WD`", <Western Digital Technologies, Inc>
- "SAMSUNG", <SAMSUNG ELECTRONICS CO. LTD>
- "`WDC WD`", <Western Digital Technologies, Inc> additional vendor specific checks used (spawns two subclasses)
- <Seagate Technology>

The plugin version 4 is more complex and can reprogram 12 drive "categories".



```
 <╥♥         ☺   ↑] Ç☺   $\ Ç☺   └\ Ç☺   î] Ç☺   ,± Ç☺   ,± Ç☺   \c Ç☺   ,b Ç☺   ┐b Ç☺
 "♣ô↓☺   Φ╧♥          ♥   1╥♥          ☺   "♣ô↓☺   Φ╧♥          ♥   ö╥♥          ☺   @d Ç☺
 b ♥Ç☺   ¼c Ç☺   Çe Ç☺   îd Ç☺   ,e Ç☺   xe Ç☺   SAMSUNG UNG     "♣ô↓☺   └╥♥          ♥
 └╥♥         ☺   (h Ç☺   Σe Ç☺   ƒg Ç☺   ä♣☺Ç☺   "♣ô↓♣   ♦╟♥          ♂   ,╟♥          ☺
 WDC WD  WD      "♣ô↓☺   £╟♥          ♣   ¼╟♥          ☺   ExcelStor tor   HDT HDT
 HDS HDS         HTE HTE         HTS HTS         Hitachi chi     IBM IBM         IC YI
 di Ç☺   êh Ç☺   ►i Ç☺   \i Ç☺   "♣ô↓☺   └╥♥          ♥   Φ╟♥          ☺   ┐j Ç☺   −i Ç☺
 dj Ç☺   ░j Ç☺   Maxtor STM STM  Max Max         "♣ô↓☺   └╥♥          ♥   ╕─♥          ☺
 ☺♥ ç₧=Q ☺♣ ƒvb→Ç*       ╟k Ç☺   ↑k Ç☺   xk Ç☺   −k Ç☺   "♣ô↓☺   └╥♥          ♥   @─♥
     ☺   ◘m Ç☺   ,l Ç☺   ╜l Ç☺   ≡╢ Ç☺   SEAGATE ST   ST Maxtor STM STM  ST iST   "♣ô↓☺
 └╥♥          ♥   1─♥          ☺   hn Ç☺   hm Ç☺   ╕n Ç☺   `n Ç☺   "♣ô↓☺   á─♥          ♥
 ¿=♥          ☺   WDC WD  WD      "♣ô↓☺   └╥♥          ♥   └─♥          ☺   do Ç☺   ╙n Ç☺
 ↑o Ç☺   ►╥ Ç☺   "♣ô↓☺   └╥♥          ♥   ╫♥           ☺   ☺◘ ↑¥φ╓o|w'▒    ☺◘ ╞Pê91KO╕╧
 ☺♦ ←|╥Gs        ☺♦ "üÅ┌*        └p Ç☺   −o Ç☺   Çp Ç☺   ╟p Ç☺   "♣ô↓☺   └╥♥          ♥
 @╫♥          ☺   ♦r Ç☺   4q Ç☺   ╕q Ç☺   4╜ Ç☺   "♣ô↓☺   └╥♥          ♥   1╫♥          ☺
 4s Ç☺   dr Ç☺   ar Ç☺   ,s Ç☺   TOSHIBA M A M   "♣ô↓☺   └╥♥          ♥   ÿ╫♥          ☺
 Dt Ç☺   ös Ç☺   ≡s Ç☺   <t Ç☺   ST ╫ST  "♣ô↓☺   └╥♥          ♥   ─╫♥          ☺   Çt Ç☺
 "♣ô↓☺   ∞╫♥          ♦   ⁿ╫♥          ☺           Xv Ç☺   ↑u Ç☺   ,± Ç☺   ,± Ç☺   ,± Ç☺
 ,± Ç☺   ,± Ç☺   0u Ç☺   (u Ç☺   └u Ç☺   "♣ô↓☺   £╟♥          ♣   4╧♥          ☺   "♣ô↓☺
```

Plugin version 4 infection "capabilities" table

Andy Rubin Android Creator Is Inventing A High-End Smartphone

How To add hashtags to notes in MacOS

New wave of ransomware exploits a vulnerability in Gigabyte drivers to ... New Ransomware Attacks Install Malicious Gigabyte Drivers To Disable Antivirus ... This second driver then goes to great lengths to kill processes and .... Ransomware installs Gigabyte driver to kill antivirus products ... Hackers exploit a vulnerability in this legitimate driver to gain kernel access. ... from starting) and Nemty (which shuts down antivirus process using taskkill utility).. Titre, RobbinHood ransomware exploit GIGABYTE driver flaw to kill ... are exploiting a vulnerable GIGABYTEÂ driver to kill antivirus products. Percona Live Europe 2018 – Save the Date!

BlazeVideo SmartShow 1.4.0.0 Full + Serial

RobbinHood Ransomware Exploits GIGABYTE Driver to Kill AV Processes.... Security researchers observed the RobbinHood ransomware family abusing a ... in a signed Gigabyte driver to circumvent security products on an infected machine. ... driver capable of killing processes associated with security products. ... for its own driver, the ransomware exploited the privilege escalation .... RobbinHood Ransomware Abuses Gigabyte Driver to stop Antivirus ... However, due to poor handling of the vulnerability by Gigabyte exploitation of the ... designed to kill processes so that encryption can occur unhindered.. According to cybersecurity firm Sophos, RobbinHood ransomware has been ... the flaw that the ransomware group is now exploiting, according to Sophos. ... use this new driver first patch the Windows kernel in-memory and kill antivirus ... TSMC to Hire 4000 Employees This Year for Process Development.. Internet & Technology News GIGABYTE Driver exploited by ransomware to kill AV Processes.. The attackers behind the RobbinHood Ransomware are exploiting a vulnerable GIGABYTE driver to install a malicious and unsigned driver ... 3d2ef5c2b0 Window 7 32bit product key

3d2ef5c2b0

How to Fix Deep Sleep Issue on Samsung Galaxy Phones